TASK ORDER
GSQ0014AJ0058

Mod PS26
CDM Dashboard

in support of:

U.S. Department of Homeland Security

Issued to:

Metrica Team Venture
100 N.E. Loop 410
Suite 520
San Antonio, TX 78216-3456

Contract GS-06F-0640Z

issued by:
The Federal Systems Integration and Management Center (FEDSIM)
1800 F Street NW, Suite 3100
Washington, DC 20405

March 3, 2014

FEDSIM Project Number 12083HSM

C.1 BACKGROUND

Cyber attacks on Federal networks are growing in numbers and becoming increasingly sophisticated, aggressive and dynamic. In 2011, the Federal Government responded to more than 107,000 attacks including cyber exploits that injected viruses, stolen information, or disrupted Federal network operations. In contrast, the decade old security regulations require manually testing major systems just once every three years, resulting in compilation of three-ring binder findings that are often out of date before they can be printed.

The security community recognized several years ago that a static approach to information assurance was inadequate. Since that time, the Federal Government has initiated a number of activities under the title "Continuous Monitoring" to improve the situation. Accordingly, various approaches toward continuous monitoring are being developed by agencies.

There are different levels of maturity in continuous monitoring across the Federal enterprise. The different approaches complicate the efforts to measure progress on a Federal enterprise level. Several Federal agencies have had isolated success. In 2008, the Department of State began a program to utilize sensors, in combination with a dashboard solution, to identify and fix cyber vulnerabilities on their networks. This program achieved a dramatic measured risk reduction (in terms of system vulnerabilities) of 20 times in just two years. Leveraging this success, the Department of Homeland Security (DHS) Continuous Diagnostics and Mitigation (CDM) program is strongly influenced by the State Department program. The DHS Continuous Diagnostics and Mitigation (CDM) program provides tested continuous monitoring, diagnosis, and mitigation capabilities designed to strengthen the security posture of the Federal civilian .gov networks.

The objective of the CDM dashboard function is to provide consistent, timely, targeted, and prioritized information to security decision-makers from cross-department, agency and Federal-level managers to systems administrators to identify and support fixing the worst problems first. The goal is to mitigate these risks before they can be exploited and cause harm to the Department and Agency (D/A) IT assets, business assets, or mission. The objectives of the CDM Dashboard initiative will be achieved by:

1. Receiving/collecting data from the D/A-level dashboards.
2. Facilitating the risk management process.
3. Reporting results to appropriate officials through a web-based user interface, organizationally-defined reports, and ad hoc query and reporting tools.

Federal Information Security Management Act (FISMA) compliance reporting mandated by the Office of Management and Budget (OMB) can be achieved through the use of Asset Summary Results (ASR) and Security Content Automation Program (SCAP) protocols for IT asset information as defined by the National Institute of Standards and Technology (NIST). The D/As will establish the communication between the Federal Level CDM Dashboard and Dashboards at other levels to report enterprise security posture information using an ASR-encapsulated summary of results.

The Dashboards will be used to automate FISMA compliance reporting mandated by OMB, including reporting through CyberScope. This reporting can be achieved through the use of NIST-defined ASR and SCAP protocols for IT asset information. The D/As will use the communication between the D/A Level and Federal Level Dashboards to report enterprise security posture information using an ASR-encapsulated summary of results. The CDM Dashboard solution will be Sensitive but Unclassified (SBU) and must be accredited as High Confidentiality, High Integrity, and Moderate Availability.

C.1.1 PURPOSE

Under the CDM program, DHS will centrally oversee the procurement, operations, and maintenance of diagnostic sensors (tools) and dashboards deployed to each agency. Using input from the sensors and agency-level CDM dashboards, Officials at each agency will be able to quickly identify which problems to fix first and empower technical managers to prioritize and mitigate risks. In addition, DHS will maintain a Federal level CDM Dashboard taking input from the agency-level dashboards, to provide situational awareness on a Federal level.

Under this procurement, GSA on behalf of DHS is commissioning the creation of an IT solution known as the “CDM Dashboard.” To that end, this procurement will obtain software design and development services and software/hardware for a series of Dashboard releases, or instances. DHS has the further strategic goal of implementing the completed CDM Dashboard use cases to other Federal agencies to manage and report their vulnerability to cyber-attacks; however, the only implementation in scope of this procurement is the Federal use case. The Dashboard created under this procurement will be used to automate FISMA compliance reporting mandated by OMB, including reporting through the currently used FISMA reporting tool, CyberScope. The Contractor shall design, develop, and support the Federal implementation of the Dashboard solution. Implementation (of the CDM Dashboard solution developed under the efforts of this procurement) at individual D/As implementation will be handled by CMaaS vendors in separate acquisitions. While the actual integration will not be performed under this task order, the contractor shall provide on-going support to CMaaS vendors to maintain and improve the functional processes within Dashboard software, to include: analysis, DHS system engineering lifecycle (SELC) reviews, software development, testing, security accreditation support, implementation support (to include acquiring property), maintenance, documentation, configuration management, Tier 3 support, training, customer relationship management, transition to support, and acquisition milestone tracking. The progression of the functionality of the Dashboard under this Task Order will be done incrementally over multiple software releases.

C.1.2 AGENCY MISSION

For this specific acquisition, the DHS strategic goal is to purchase an integrated, hierarchical Dashboard solution, to implement the Federal use case, and to make the Dashboard capability available to DHS and Federal agencies to manage and report their vulnerability to cyber-attacks.

C.1.3 CDM Dashboard Terminology and Architecture

This section describes the dashboard's terminology and includes an architectural diagram of the proposed dashboard hierarchy. This terminology will be used throughout this Task Order Request and during the execution of these requirements.

C.1.3.1 CDM Dashboard Terminology

DASHBOARD

The term *Dashboard* is used in the context of the CDM Program to refer to all parts of the Continuous Asset Evaluation, Situational Awareness and Risk Scoring Reference Architecture Report (**CAESARS**) architecture except the sensor sub-system. The CAESARS was published by DHS in 2010 and available at http://www.dhs.gov/xlibrary/assets/fns-caesars.pdf. The term Dashboard addresses the remaining parts of the CAESARS architecture: Database/Repository, Analysis/Risk Scoring, and Presentation and Reporting. CDM dashboards are arranged in a hierarchy. Each dashboard will be an independently executing application with its own inputs and outputs. The dashboards may be technically equivalent but will function differently based on their position in the hierarchy. DHS will deploy a hierarchical CDM Dashboard solution at DHS and at the D/As. There are four tiers of dashboard deployment, corresponding to four hierarchy locations. Those D/As that currently have existing legacy applications that are also known as "dashboards" but provide functionality not specific to CDM capabilities will be able to keep them but will also be required to utilize the CDM Dashboard solution. Existing D/A legacy dashboards are unrelated to this effort. The CDM Dashboard assumes that all data it receives is normalized and SCAP compliant. It is the responsibility of the sensor layer within the CAESARS Framework to perform this function.

The **Federal Level CDM Dashboard** displays summary CDM data for the entire Federal Government. This dashboard will be used by oversight groups, e.g., Offices of Inspector Generals, to monitor Government-wide risk. Implementation of this CDM Dashboard will be the responsibility of the CDM Dashboard vendor.

An **Intermediate Summary CDM Dashboard** is an instance of the DHS-provided D/A solution that obtains all of its data from other D/A dashboards, and all of whose data is at a summary level (no object-level data). Implementation of this CDM Dashboard will be the responsibility of the CMaaS vendor, D/A, or other third party vendor.

Only other Summary CDM Dashboards and/or the Federal Level CDM Dashboard may exist above this level in the hierarchy. This type of dashboard would be used to summarize data for a large D/A where object-level data is not required/ permitted.

An **Intermediate Object-Level CDM Dashboard** is an instance of the DHS-provided D/A solution that obtains all of its data from other D/A dashboards, but some of whose data is at the object level.

Only base (see below) and/or other Intermediate Object-Level Dashboards may exist below this dashboard. This type of dashboard would be used if multiple Base Dashboards are needed (for performance reasons, for example) for a D/A, and the D/A still wants/permits detailed data at the D/A level. It can have all the functionality of a Base CDM Dashboard except that which requires connection to sensors. (Functionality related to these missing items is turned off).

In general, Intermediate-level dashboards are for use by D/As and/or their sub-components to monitor the risk associated with their organizational scope. If the dashboard is object-level, then it will also facilitate identification and removal of specific defects on specific objects. Implementation of this CDM Dashboard will be the responsibility of the CMaaS vendor, D/A, or other third party vendor.

A **Base CDM Dashboard** is an instance of the DHS-provided D/A solution whose data is obtained directly from sensors. Each Base CDM Dashboard must be capable of obtaining data, directly or indirectly, from each of the sensors that monitor the network for the data specified in the CDM Program and for the objects within the dashboard's scope via a database.

A Base CDM Dashboard will be used by organizations that own the objects in the scope of the dashboard, not only to monitor risk but to facilitate identification and removal of specific defects on specific objects.

CDM Dashboards will be connected through a hierarchy, with the Federal Dashboard at the top. Higher level dashboards will be capable of transferring meta-data to lower level dashboards. Lower level dashboards will be capable of passing data to the adjacent higher level dashboard. The aggregation process is needed by both small and large D/As. Large D/As may have multiple enclaves, each of which must have its own dashboard. The Government seeks to summarize the data up to and including the Federal level, which includes all executive branch civilian D/As**.** Implementation of this CDM Dashboard will be the responsibility of the CMaaS vendor, D/A, or other third party vendor.

RISK SCORES

A *risk score* for an individual defect is a numerical representation of the relative severity or importance of the finding to the risk for the system as a whole. Standardized scoring systems have been created for vulnerabilities (CVSS) and software weaknesses (CWSS); they have also been developed for configuration settings (CCSS), but these are not yet as widely accepted. Standardized scoring systems do not yet exist for other types of findings, such as unauthorized/unmanaged hardware, unauthorized software, anti-virus protection weaknesses, or data loss. A risk score for an IT asset represents the total measurable security risk associated with that asset. It combines standardized and non-standardized metrics with management heuristics and weightings to estimate the magnitude of risks and prioritize the allocation of resources for risk remediation. Risk scoring is a key element of the dashboard function, because it provides fair, objective, and repeatable quantitative comparisons among security risk elements that are not inherently comparable.

The lowest level scores are at the object/defect level. These can be summed to get the score for an object, the score for a defect across the entire D/A, or the total score for all objects in the D/A.

Each dashboard defines arbitrary groupings appropriate to the level of detail of its data and then report scores or findings by a selected grouping. Groupings of objects are used to assign risk scores to the sub-organizations that are directly responsible for, and able to actually remediate, findings. Groupings of defects facilitate their analysis prior to selection for remediation, Each dashboard aggregates scores across any of the groupings to facilitate analysis for prioritization. Each dashboard calculates average risk scores and converts them into risk levels, e.g., letter grades, for appropriate groups of devices/objects, and provides group rankings based on average risk score compared to various reference groupings.

An aggregation process is needed by both small and large D/As, ranging from several hundred objects to millions of objects. Large D/As may have multiple enclaves and may want to operate the security configuration compliance assessment at the enclave level. Ultimately, the Government seeks to summarize the data up to and including the Federal level, which includes all civilian executive D/As**.** The lowest level of detail required for the Federal Dashboard is aggregate scores for object groups by defect check, e.g., the total score for all objects in a sub-organization for a specific vulnerability on a specific software product.

SITES

For a dashboard that contains data at the object level (Base and Intermediate Object-level CDM Dashboards), the objects should be organized into object containers called *sites* such that every object is in exactly one site. The scores assigned to the objects will be combined to provide a single score for the entire site. A site is intended to represent administrative ownership – the owner of the site is responsible for fixing the security issues associated with the site’s objects. The case where responsibility for an object’s scores is split among multiple owners is addressed by risk transfers.

SCORE TYPES

Scores are defined by sets of scoring parameters and are meant to be used by D/As to help prioritize the work of mitigating security defects. Each D/A must be able to tailor the scoring parameters to best accomplish this. However, at the Federal level, scores are meant to be used to assess the security posture of all the D/As and therefore the same scoring parameters must apply to all D/As. This is accomplished by using two separate sets of scoring parameters (one mandatory set for Federal scores and one optional set for D/A scores) throughout, although some D/As may wish to simply use the Federal parameters. Local D/A scoring, if desired, each D/A can assign these scores in whatever way meets their objective for using local scores, including different scores for different enclaves.

Scores are defined by sets of scoring parameters and are meant to be used by D/As to help prioritize the work of mitigating security defects. Each D/A must be able to tailor the scoring parameters to best accomplish this. However, at the Federal level, scores are meant to be used to assess the security posture of all the D/As and therefore the same scoring parameters must apply to all D/As. This is accomplished by using two separate sets of scoring parameters (one mandatory set for Federal scores and one optional set for D/A scores) throughout, although some D/As may wish to simply use the Federal parameters. If desired, each D/A can assign these scores in whatever way meets their objective for using local scores, including different scores for different enclaves.

The general scoring algorithm includes factors that take into account vulnerability score, threat multipliers, and impact multipliers. When using scores to evaluate risk, the inclusion of threat and impact is always appropriate. However, when using scores to grade performance, some multipliers may introduce perverse incentives and/or unfairness (particularly if local managers cannot mitigate the extra threat or impact), so the flexibility to ignore such multipliers may be useful. The dashboard should distinguish two kinds of "multipliers" (for both threat and impact): grade-relevant multipliers and non-grade-relevant multipliers. This produces two versions of the Federal and Local Scores: 1) a Grading Score (ignores the non-grade-relevant multipliers), and 2) a full-risk-score (includes all multipliers). The terminology shown on dashboard screens and reports these scoring types must be configurable to mitigate possible confusion with other D/A terminology. An end user must at any time be able to select display of scores using one of four scoring types: a) Federal-grading, b) Federal-Full-Risk, c) Local-grading, and d) Local-Full-Risk.

RISK TRANSFERS

To ensure that prioritization is limited to risks that can be directly remediated by the assigned organization, risk scores must be transferrable from one sub-organization to another at the object-defect level. For example, if an upgrade of a vulnerable version of Java Runtime Environment would break an application managed by another organization, the risk score for that vulnerability should be transferred to the organization that owns the application for every host that is used to run that application. Definition/approval of risk transfers is the responsibility of the D/A. Implementation of transfer rules is the responsibility of the D/A, who may delegate this to the CMaaS Contractor. Note that the dashboard must allow a D/A user to successfully implement risk transfers if they choose to do so. Risk Transfers are absolutely essential to maintaining a risk monitoring environment where risks can be fairly prioritized by the organizational level that is able to remediate the problems.

DEFECT

A *defect* is a security-related condition that represents a difference between a desired state and an actual state, e.g., a specific vulnerability in a software product or a user password set to never expire.

OBJECT

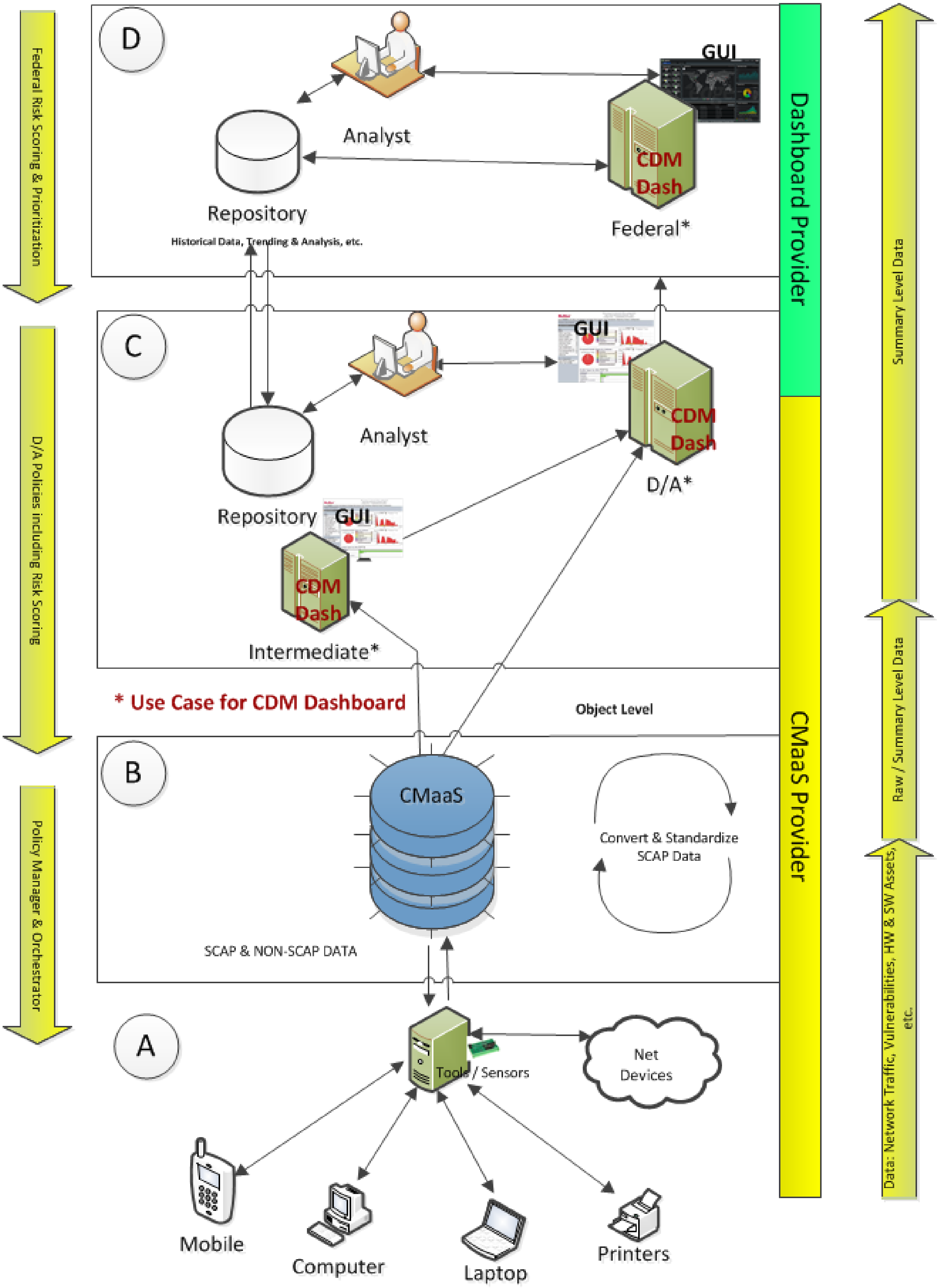
An *object* is anything that can have a defect. Generally, it is understood that an object is a network end point, e.g., a server, router, or workstation. However, a directory account will also be considered an object. In addition, objects form a hierarchy, i.e., one object can be contained in another object. For example, each software product installed on a server will be considered an object, but all such objects on a given server are contained in the object representing the server. Objects that are not contained within other objects will be called *root objects* where the distinction is important.

SENSOR

The term *sensor*, as used throughout this TOR, refers to the collection subsystem in the CAESARS-Framework Extension. The sensor concept includes both tools that collect data about endpoints on the network and the possibility of manually input data.

C.1.3.2 CDM Dashboard Architecture

The figure below shows the hierarchy possibilities.


Federal Risk Scoring & Prioritization
D/A Policies including Risk Scoring
Policy Manager & Orchestrator
D
Analyst
GUI
Repository
Historical Data, Trending & Analysis, etc.
CDM Dash
Federal*
C
Analyst
GUI
Repository
GUI
CDM Dash
D/A*
CDM Dash
Intermediate*
* Use Case for CDM Dashboard
Object Level
B
CMaaS
Convert & Standardize SCAP Data
SCAP & NON-SCAP DATA
A
Tools / Sensors
Net Devices
Mobile
Computer
Laptop
Printers
Dashboard Provider
CMaaS Provider
Summary Level Data
Raw / Summary Level Data
Data: Network Traffic, Vulnerabilities, HW & SW Assets, etc.

C.2 SCOPE

This procurement will obtain a single hierarchical CDM Dashboard solution with multiple use cases (Top/Federal Level, Intermediate Summary Level, and Intermediate Object Level). The Contractor shall design, develop, and support the implementation of a Dashboard Solution Interim Operating Capability (IOC) at the D/A levels (Intermediate Summary Level, and Intermediate Object Level); to a Full Operating Capability (FOC) for the Federal and all D/A level CDM Dashboards. The Contractor shall provide: analysis, DHS system engineering lifecycle (SELC) reviews, software development, testing, security accreditation support, implementation support (to include acquiring property), maintenance, documentation, configuration management, Tier 3 support, training, transition to support, and acquisition milestone tracking. The contractor will only implement the Federal use case of the CDM Dashboard, all other use cases will be implemented by CMaaS vendors. However, insofar as the Dashboard solution includes commercial or open-source software, the Contractor shall also provide to the Government, as part of this procurement, licenses to such commercial or open-source software in quantities sufficient both for the Federal implementation and to enable the Government to later provide such licenses to the CMaaS vendors for D/A implementations. Aspects of the CDM are classified TS/SCI and the contractor personnel supporting Task 5 – FOC Dashboard Implementation, of this effort will be required to work within classified space, handle TS/SCI Material, and participate in the TS/SCI efforts.

C.3 OBJECTIVES

The objectives of this Task Order (TO) are to develop an IOC and FOC tiered hierarchical dashboard capability for the Federal Government. DHS requires the pilot of the IOC at the D/A levels during CY 2014. The progression from IOC to FOC implementation may be done incrementally occurring over several software releases. Additionally, the FOC version is expected to have a software refresh cycle of every six months.

C.4 TASKS

C.4.1 TASK 1 – PROVIDE PROGRAM MANAGEMENT (CLIN X001)

The Contractor shall provide program management support under this TO from TO Award (TOA) and project kick-off through transition-out. This program management shall include status reporting, status meetings, Project Management Plan, trip reports, Quality Control Plan, and Earned Value Management.

This includes the management and oversight of all activities performed by Contractor personnel, including sub-Contractors, to satisfy the requirements identified in this Statement of Work (SOW). The Contractor shall identify a Program Manager (PM) by name who shall provide management, direction, administration, quality control, and leadership of the execution of this TO. The Contractor shall schedule meetings and provide deliverables in accordance with Section F.

C.4.1.1 SUBTASK 1.1 – COORDINATE A PROJECT KICK-OFF MEETING

The Contractor shall schedule and coordinate a Project Kick-Off Meeting at the location approved by the Government. The meeting will provide an introduction between the Contractor personnel and Government personnel who will be involved with the TO. The meeting will provide the opportunity to discuss technical, management, and security issues, and travel authorization and reporting procedures. The attendees shall include vital Contractor personnel, representatives from the directorates, other relevant Government personnel, and the FEDSIM COR. The Contractor shall provide the following at the Kick-Off meeting:

1. Project Management Plan (PMP)
2. Updated Quality Control Plan (QCP)
3. Updated Earned Value Management (EVM) Plan.

C.4.1.2 SUBTASK 1.2 – PREPARE A MONTHLY STATUS REPORT (MSR)

The Contractor PM shall develop and provide an MSR (Section J, Attachment B) using Microsoft (MS) Office Suite applications, by the tenth of each month via electronic mail to the Federal Network Resilience (FNR) Technical Point of Contact (TPOC) and the COR. The MSR shall include the following:

1. Activities during reporting period, by task (include: on-going activities, new activities, activities completed; progress to date on all above mentioned activities). Start each section with a brief description of the task.
2. Problems and corrective actions taken. Also include issues or concerns and proposed resolutions to address them.
3. Personnel gains, losses, and status.
4. Government actions required.
5. Schedule (show major tasks, milestones, and deliverables; planned and actual start and completion dates for each).
6. Summary of trips taken, conferences attended, etc. (attach Trip Reports to the MSR for the reporting period).
7. EVM statistics.
8. Accumulated invoiced cost for each CLIN up to the previous month.
9. Projected cost of each CLIN for the current month.

C.4.1.3 SUBTASK 1.3 – CONVENE TECHNICAL STATUS MEETINGS

The Contractor PM shall convene a monthly Contract Activity and Status Meeting with the TPOC, COR, and other vital Government stakeholders. The purpose of this meeting is to ensure all stakeholders are informed of the monthly activities and MSR, provide opportunities to identify other activities and establish priorities, and coordinate resolution of identified problems or opportunities. The Contractor PM shall provide minutes of these meetings, including attendance, issues discussed, decisions made, and action items assigned, to the COR within five workdays following the meeting.

C.4.1.4 SUBTASK 1.4 – PREPARE A PROJECT MANAGEMENT PLAN (PMP)

The Contractor shall document all support requirements in a PMP. The PMP shall:

1. Describe the proposed management approach
2. Contain detailed Standard Operating Procedures (SOPs) for all tasks
3. Include milestones, tasks, and subtasks required in this TO, to include granular detail, and all reoccurring deliverables (i.e. "New Code" and "Customizations", as defined in section C.4.12)
4. Provide for an overall Work Breakdown Structure (WBS) and associated responsibilities and partnerships between or among Government organizations
5. Include the Contractor's QCP and EVM Plan.

The Contractor shall provide the Government with a draft PMP at the project Kick Off meeting, on which the Government will make comments. The final PMP shall incorporate the Government's comments.

C.4.1.5 SUBTASK 1.5 – UPDATE THE PROJECT MANAGEMENT PLAN (PMP)

The PMP is an evolutionary document that shall be updated annually and at the incorporation of any major task order modification. The Contractor shall work from the latest Government-approved version of the PMP.

C.4.1.6 SUBTASK 1.6 – PREPARE TRIP REPORTS

The Government will identify the need for a Trip Report when the request for travel is submitted. The Contractor shall keep a summary of all long-distance travel including, but not limited to, the name of the employee, location of travel, duration of trip, and point of contact (POC) at travel location.

C.4.1.7 SUBTASK 1.7 – UPDATE QUALITY CONTROL PLAN (QCP)

The Contractor shall update the QCP submitted with their proposal and provide a final QCP as required in Section F. The Contractor shall periodically update the QCP, as required in Section F, as changes in program processes are identified by the Government.

C.4.1.8 SUBTASK 1.8 - EARNED VALUE MANAGEMENT (EVM)

The Contractor shall employ and report on EVM in the management of this TO. See H.19, Earned Value Management**,** for the EVM requirements.

C.4.1.9 SUBTASK 1.9 – TRANSITION-OUT

The Transition-Out Plan shall facilitate the accomplishment of a seamless transition from the incumbent to an incoming Contractor/Government personnel at the expiration of the TO. The Contractor shall provide a Transition-Out Plan NLT 90 calendar days prior to expiration of the TO. The Contractor shall identify how it will coordinate with the incoming Contractor and/or Government personnel to transfer knowledge regarding the following:

1. Project management processes.
2. Points of contact.
3. Location of technical and project management documentation.
4. Status of ongoing technical initiatives.
5. Appropriate Contractor–to-Contractor coordination to ensure a seamless transition.

6. Transition of Key Personnel.
7. Transfer of Software Licenses.
8. Schedules and milestones.
9. Actions required of the Government.

The Contractor shall also establish and maintain effective communication with the incoming Contractor/Government personnel for the period of the transition via weekly status meetings.

C.4.2 TASK 2 – IOC Analysis of Design Alternatives (CLIN 0002)

Within four months of award the Contractor shall analyze at a minimum three alternative Commercial off-the-Shelf (COTS) or Open Source products that can meet as many of the IOC Dashboard requirements as possible for, at a minimum, the Base use case (see Section J, Attachments P and I). The IOC solution shall be based on COTS or Open Source product(s). The Contractor shall conduct an analysis of IOC Design Alternatives to include:

1. An analysis of dashboard requirements.
2. A gap analysis between the continuous monitoring information management needs for risk prioritization and reporting and the Government's current capabilities.
3. An analysis of existing dashboards and where they do not meet CDM reporting requirements, research potential incompatibilities, analyze system interfaces, and propose ways to resolve potential interface conflicts.
4. A comparison of alternative solutions and their capabilities for dashboard development and implementation (identifying Federal enterprise architecture constraints, if any).
5. A report that addresses at a minimum, the impacts on costs, engineering trade-offs, cost/benefit analysis, schedule dependencies, and technically feasible alternative approaches.
6. Exploration of possible solutions with the goal of identifying whether the required IOC dashboard capabilities currently exist in a commercial product, whether it exists but needs enhancements..
7. Sound rational for recommended approach.
8. Sound rational for rejection of alternatives.
9. Briefing for IOC Decision.

The Government will determine the best solution, based on the Contractor's analysis and recommendations. Once the decision is made, the Contractor shall create a written report on Design Alternatives and prepare an information briefing to be presented to DHS and D/A decision makers.

C.4.3 TASK 3 – Initial Operating Capability (CLIN X001)

The Contractor shall develop/procure an Initial Operating Capability (IOC) for the D/A level Dashboards. The IOC shall be based on Government selected solution from Task 2. It shall be used to provide an initial dashboard capability while the Full Operating Capability (FOC) D/A level and Federal Dashboards are being developed

C.4.3.1 SUBTASK 3.1 – IOC Systems Engineering Life Cycle (SELC) Compliance

The Contractor shall perform all systems engineering, architecture and testing tasks in this SOW in accordance with DHS AD 102-01/SELC. The Contractor shall provide best practices, technologies, tools, and support to quality and operational assessments, integration testing and system test and evaluation, including development of security certification and accreditation packages for agencies for the dashboards. DHS, with vendor support, will develop one package that can be provided for all D/A's to use. All development and testing will take place at the vendors facilities, utilizing the vendors equipment with Government access to the location and all artifacts made available to the Government. If required, the Contractor shall participate in and support an IV&V to ensure the monitoring and evaluation of projects through activities such as, but not limited to, assessments, process and procedure audits, project and performance management, and systems analysis and design. IV&V testing shall be in accordance with the DHS SELC.

The DHS SELC framework is used across all DHS systems; it will be the only SELC framework model to be followed. DHS may elect to have stakeholders from D/A as participants in the various reviews, most likely the Operational Readiness Reviews into their environment.
It consists of nine process stages and corresponding Systems Engineering Reviews: Solution Engineering, Planning, Requirements Definition, Design, Development, Integration & Test, Implementation, Operations & Maintenance, and Disposition. SELC stage entry and exit criteria completion (as well as technical progress) are validated in the stage reviews. Solution Engineering focuses on enterprise level activities. The remaining stages address project and system related activities. The Contractor shall provide support across all phases of the SELC, including engineering review and SELC stage specific activities as required.

The stages and reviews may be repeated by projects during capability implementation. The stages and activities may be tailored by the program, as not all projects will require all stages in the SELC and others may require multiple iterations. Minor system modifications and enhancements during O&M will not require all stages of the SELC to be performed. Major enhancements will be treated as new projects within the SELC.

The Contractor shall follow a tailored approach to the acquisition milestone review process, in accordance with DHS Acquisition Directive 102-01.

The Contractor shall produce DHS SELC Documentation and Briefing Materials and participate in the following four design reviews for the IOC Dashboard.

1. Solution Engineering Review (SER),
2. Project Planning Review (PPR),
3. Critical Design Review (CDR), and
4. Production Readiness Review/Operational Test Readiness Review (PRR/OTRR).

C.4.3.2 SUBTASK 3.2 – Provide the IOC Solution for D/As

The Contractor shall implement the Initial Operating Capability. This implementation shall include Systems Engineering Life Cycle Compliance, DHS Enterprise Architecture Compliance, Security Accreditation, Maintenance Support, and Dashboard IOC Documentation. The Contractor shall provide the following:

1. Provide and tailor the Government-approved dashboard solution.
2. Perform reviews to identify technical and operational issues and problems such as requirements definition, architecture and policy compliance, and engineering guideline development including peer-to-peer reviews, code walk-throughs, and formal design reviews.
3. Recommend opportunities for resolving issues in requirements, data, applications, and infrastructure elements.
4. Coordinate with the CMaaS Contractor(s) or other Government-designated integrators for the engineering and integration of the Dashboard solution with computer system, hardware, operating software, and networks.
5. Provide analysis, modeling, design, development, enhancements, testing, and documentation of new and existing capabilities. The Dashboard solution shall be subject to formal Government and end-user acceptance test in accordance with approved test plan and procedures (which shall be consistant with the CDM Test Evaluation Master Plan (TEMP) definitions.
6. Conduct an extended development test (EDT) within a DHS supplied environment prior to completion of the production-ready D/A Dashboard solution.
7. Production ready IOC solution is handed off to CMaaS vendor for implementation.
8. After the IOC Dashboard solution is operational, the Contractor shall provide enhancements to existing software application programs throughout the period of performance; develop work-arounds to the IOC Dashboard based on Government approved requirements; and provide a software release every 6 months until FOC is achieved.

The Contractor shall establish associate Contractor agreements with the CMaaS Contractor(s) or other integrator for cooperative co-maintenance of dashboard software. Object containers, object types, defect checks and defect groups can all be defined locally, as can scoring parameters. Impact factors can be defined at the object level even if local scoring is not used. Additional user-level customizations may be required at individual D/As.

C.4.3.3 SUBTASK 3.3 – IOC Security Accreditation

The IOC Dashboard solution will be a DHS asset. The DHS will perform the security accreditation and the D/A will perform a risk acceptance. The Contractor shall provide input and facilitate the execution of Memoranda of Agreement (MOAs) between DHS and the D/A for risk acceptance in a support capacity to DHS. The Contractor shall ensure that C&A is received from DHS before the IOC capability is installed on a DHS network. The Contractor shall provide all support required to ensure that the Dashboard passes the DHS security accreditation process. The IOC Dashboard shall be subject to continuous monitoring and reaccreditation every three years. The Contractor shall support the third party performance of the security accreditation tests against the system. The Contractor shall ensure that the IOC Dashboard solution remains accredited in accordance with DHS security guidelines (4300 A, DHS Sensitive Systems guidelines). The Contractor shall perform the following security authorization tasks:

1. Provide the necessary support for security authorization of the Federal Dashboard community.
2. Provide support for the DHS accreditation process in accordance with applicable DHS standards.
3. Prepare documentation in support of the DHS accreditation process.

C.4.3.4 SUBTASK 3.4 –IOC Maintenance Support

The Contractor shall establish and manage a comprehensive Maintenance Program that includes IOC Dashboard solution installation support, connections, access control, configurations and inventory of components. The Contractor shall provide comprehensive support, including:

1. Dashboard policies, procedures, and guidance.
2. Dashboard implementation packages and guidance.
3. Scheduled maintenance.
4. Unscheduled maintenance.
5. COTS/OPEN SOURCE CODE Product upgrades.
6. Planned and integrated logistics support for Dashboard components.
7. Integration of new technology.
8. Information security.

D/A level dashboard software and hardware will be installed and integrated by CMaaS Contractor(s) or other Government-designated integrators and the Dashboard Contractor shall provide technical advice and support as needed.

C.4.3.5 SUBTASK 3.5 – IOC DHS Enterprise Architecture Compliance

To the maximum extent possible, the Contractor's IOC Dashboard solution shall meet DHS Enterprise Architecture policies, standards, and procedures. However, the mission of the CDM program is to service the entire Federal Executive Civilian branch (.gov Domain), and its Enterprise Architecture requirements must be viewed from that broader perspective. As such, there may be instances in which the CDM Architecture may need to deviate from and/or extend Homeland Security (HLS) Enterprise Architecture (EA) requirements. The Contractor shall comply with the following Homeland Security (HLS) EA requirements with regard to the IOC Dashboard:

1. The IOC D/A dashboard shall be compliant with the Federal enterprise architecture. Specific compliance issues should be treated as a defect to be considered for the next release.
2. IT hardware and software deployed on DHS networks shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
3. Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.

4. Development of data assets, information exchanges and data standards shall comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts shall be developed and validated according to DHS data management architectural guidelines.
5. Applicability of Internet Protocol Version 6 (IPv6) to DHS-related elements (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

C.4.3.6 SUBTASK 3.6 – IOC Dashboard Documentation

All IOC Dashboard software releases shall be accompanied with documentation updates including Release Notes and Release Implementation Guidelines, page updates (one copy per site) and paperless electronic on-line Dashboard User Manual, and Operations Manual updates. The Release Notes and Release Implementation Guidelines shall include descriptions of what has changed in the new release and how to install the new release(s), including installation requirements for particular sites. The documentation shall include a description of functional changes for all releases. The Contractor shall provide the documentation in coordination with scheduled block release dates.

C.4.4 TASK 4 – FOC Requirements Validation and Design Alternatives (CLIN X003)

Within 12 months of award the Contractor shall validate the Dashboard solution requirements and develop FOC design alternatives for Government decision.

C.4.4.1 SUBTASK 4.1 – FOC Requirements Validation

The Contractor shall conduct an analysis and document validation activities that include, but are not limited to, the following:

1. Analysis of the production environment (D/A CDM Dashboard connected to the live D/A feeds of their network).
2. Analysis of existing and new sensors and dashboard capabilities.
3. Analysis of system interfaces.
4. Identifying potential interface incompatibilities.
5. Resolving interface conflicts.
6. Ensuring that the Dashboard solution will meet the constraints of DHS Enterprise Architecture.

The Contractor shall compile a list of potential solutions for the FOC Dashboard requirements. Following Government review of the design alternatives, the Contractor shall procure, test and evaluate those platforms that the Government identified as best meeting its need.

C.4.4.2 SUBTASK 4.2 – FOC Design Alternatives

Based on the validated requirements in subtask 4.1, the Contractor shall design alternative approaches to meet the FOC CDM Dashboard requirements for Government selected platforms. Building on the IOC Analysis of Design Alternatives (Task 2), the Contractor shall conduct an analysis of FOC Design Alternatives to include:

1. Analytical comparison of alternative solutions and their capabilities for dashboard development and implementation.
2. Conceptual solutions with the goal of identifying whether the IOC solution needs enhancements, or if it must be a new custom developed tool that may or may not utilize portions of existing tools.
3. Rational for recommended approach.
4. Rational for rejection of alternatives.
5. Presentation of FOC Design Alternatives

After presenting the FOC Design Alternatives, the Government will make a select the solution that best meets its requirements. Once the decision is made, the Contractor shall create a written report on the FOC Design Alternatives and prepare an information briefing to be presented to DHS and D/A decision makers.

C.4.5 TASK 5 –FOC Dashboard Implementation (CLIN X001)

The Contractor shall implement the FOC Dashboard Federal use case within 24 months after approval of FOC recommendations. This implementation shall include SELC Compliance, DHS Enterprise Architecture Compliance, Security Accreditation, Maintenance Support, and Dashboard FOC Documentation. The Contractor shall provide FOC capabilities for D/A use cases, and integrate a FOC Federal use case CDM Dashboard, based on the Government's decision from the Alternatives Briefing in Task 4.2. The FOC Dashboards shall meet as many of the requirements as possible (see Section J, Attachments P and I). The Contractor shall provide software development, functionality enhancement (progressive versions), and maintenance support for Dashboard(s) as approved by the Government. The Contractor shall develop a software development process that employs best industrial practices including integration, testing, and documentation of software. Object containers, object types, defect checks and defect groups can all be defined locally, as can scoring parameters. Impact factors can be defined at the object level even if local scoring is not used. Performance on this contract will requires support personnel to access information up to and including Top Secret and Sensitive Compartmented Information (SCI). Contractor staff supporting Task 5 that will require access within the hosting environment (in relation to the Federal CDM Dashboard instance only) of this contract are required to hold and maintain a Top Secret SCI clearance.

C.4.5.1 SUBTASK 5.1 – FOC Systems Engineering Life Cycle Compliance

The Contractor shall perform all systems engineering, architecture and testing tasks in this PWS in accordance with DHS AD 102-01/SELC. The Contractor shall provide best practices, technologies, tools, and support to quality and operational assessments, integration testing and system test and evaluation, including development of security certification and accreditation packages for agencies for the dashboards. If required, the Contractor shall participate and support an IV&V to ensure the monitoring and evaluation of projects through activities such as, but not limited to, assessments, process and procedure audits, project and performance management, and systems analysis and design. IV&V testing shall be in accordance with the DHS SELC.

The DHS SELC framework is used across all DHS systems. It consists of nine process stages and corresponding Systems Engineering Reviews: Solution Engineering, Planning, Requirements Definition, Design, Development, Integration & Test, Implementation, Operations & Maintenance, and Disposition. SELC stage entry and exit criteria completion (as well as technical progress) are validated in the stage reviews. Solution Engineering focuses on enterprise level activities. The remaining stages address project and system related activities. The Contractor shall provide support across all phases of the SELC: including engineering review and SELC stage specific activities as required.

The stages and reviews may be repeated by projects during capability implementation. The stages and activities may be tailored by the program, as not all projects will require all stages in the SELC and others may require multiple iterations. Minor system modifications and enhancements during O&M will not require all stages of the SELC to be performed. Major enhancements will be treated as new projects within the SELC.

The Contractor will follow a tailored approach to the acquisition milestone review process, in accordance with DHS Acquisition Directive 102-01. For the FOC Dashboards the Contractor shall provide the documentation, briefing materials, and presentations for the following DHS SELC reviews:

1. Solution Engineering Review (SER).
2. Project Planning Review (PPR).
3. Systems Definition Review/Preliminary Design Review (SDR/PDR),
4. Critical Design Review (CDR).
5. Integration Readiness Review/Development Test Readiness Review (IRR/DTRR).
6. Production Readiness Review/Operational Test Readiness Review (PRR/OTRR).

The Contractor shall provide subject matter expertise on the FOC Dashboards for the Operational Readiness Review (ORR) and the Post Implementation Review (PIR). The actual reviews will be conducted by another Contractor tasked with installation of the FOC Dashboards.

C.4.5.2 SUBTASK 5.2 – FOC DHS Enterprise Architecture Compliance

To the maximum extent possible, the Contractor's dashboard solution shall meet DHS Enterprise Architecture policies, standards, and procedures. However, the mission of the CDM program is to service the entire Federal Executive Civilian branch (.gov Domain), and its Enterprise

Architecture requirements must be viewed from that broader perspective. As such, there may be instances in which the CDM Architecture may need to deviate from and/or extend Homeland Security (HLS) EA requirements. The Contractor shall comply with the following Homeland Security (HLS) EA requirements with regard to dashboard:

1. The developed FOC solution shall be compliant with the Federal enterprise architecture and may need to follow specific D/A EA guidelines when deployed as identified, and provided by DHS.
2. IT hardware and software to be deployed on DHS networks shall be compliant with the HLS EA Technical Reference Model (TRM) Standards and Products Profile.
3. Description information for all data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office (EDMO) for review, approval and insertion into the DHS Data Reference Model and Enterprise Architecture Information Repository.
4. Development of data assets, information exchanges and data standards will comply with the DHS Data Management Policy MD 103-01 and all data-related artifacts will be developed and validated according to DHS data management architectural guidelines.
5. Applicability of Internet Protocol Version 6 (IPv6) to DHS-related elements (networks, infrastructure, and applications) specific to individual acquisitions shall be in accordance with the DHS Enterprise Architecture (per OMB Memorandum M-05-22, August 2, 2005) regardless of whether the acquisition is for modification, upgrade, or replacement. All EA-related component acquisitions shall be IPv6 compliant as defined in the U.S. Government Version 6 (USGv6) Profile (National Institute of Standards and Technology (NIST) Special Publication 500-267) and the corresponding declarations of conformance defined in the USGv6 Test Program.

C.4.5.3 SUBTASK 5.3 – FOC Security Accreditation Support

The FOC Dashboard software will be a DHS asset. The DHS will perform the security accreditation and the D/A will perform a risk acceptance. The Contractor shall support the D/A with regard to the execution of Memoranda of Agreement (MOAs) with the D/A for risk acceptance. The Contractor shall ensure that C&A is received before the FOC capability is installed on a DHS network. The Contractor shall provide all support required to ensure that the Dashboard passes the DHS security accreditation process. The Government also expects that the FOC Dashboard, as part of a CMaaS deployment, must be subject to continuous monitoring and reaccreditation every three years. The Contractor shall run tests against the system. The Contractor shall ensure that the FOC Dashboard system remains accredited in accordance with DHS security guidelines (4300 A, DHS Sensitive Systems guidelines).

The Contractor shall perform the following security authorization tasks:

1. The Contractor shall provide the necessary support for security accreditation of the CDM Dashboard community.
2. Provide support for the DHS accreditation process in accordance with DHS standards.

3. Prepare documentation in support of the DHS accreditation process.

C.4.5.4 SUBTASK 5.4 – FOC Maintenance Support

The Contractor shall establish and manage a comprehensive Maintenance Program that includes for all use cases; connections, access control, configurations, inventory of dashboard components, and installation of the Federal CDM Dashboard use case. The Contractor shall provide comprehensive support, including:

1. Dashboard Policies, procedures, and guidance.
2. Dashboard implementation packages and guidance.
3. Scheduled maintenance.
4. Unscheduled maintenance.
5. Planned and integrated logistics support for Dashboard components.
6. Integration of new technology.
7. Information security.

D/A CDM Dashboard use cases will be installed, implemented, and operated by CMaaS Contractor(s) or other integrator(s).

C.4.5.5 SUBTASK 5.5 – FOC Documentation of Dashboard Build

All software releases shall be accompanied with documentation updates including Release Notes and Release Implementation Guidelines, page updates (one copy per site) and paperless electronic on-line Dashboard User Manual, and Operations Manual updates. The Contractor shall provide the documentation to the sites and to DHS, in coordination with scheduled block release dates. The Release Notes and Release Implementation Guidelines shall include descriptions of what is taking place in the new release and how to install the new release(s), including installation requirements for particular sites. They shall include:

1. A description of functional changes for all releases,
2. Current and new sensors and dashboards.
3. System interfaces.
4. Resolving interface conflicts.
5. Ensuring that systems meet the constraints of systems architecture(s).

C.4.6 TASK 6 – Customer Support (CLIN X001)

Customer Support shall include Tier Three help support and training support to ensure the highest state of reliability for the Federal Dashboard and related dashboards.

C.4.6.1 SUBTASK 6.1 – Tier 3 Support

The Contractor shall provide Tier Three Support for the Dashboard User Community for IOC and then FOC. The Contractor shall provide a ticketing system and hot-line capability during the normal workweek (Monday through Friday) and shall provide coverage from 0700 through 1700 hours Eastern time daily (normal work week).

1. Tier One support will be provided by the D/As. Tier One support shall include Problem resolution using standard methodologies and basic troubleshooting techniques.
2. Tier Two support will be provided by CMaaS Contractor(s) or Government-designated integrators. Tier Two support shall include more in-depth troubleshooting and shall require specialized knowledge of sensors and dashboards for remediation.
3. All calls determined by Tier Two to be related to the dashboard solution and not resolved through Tier Two shall be forwarded to the Dashboard Contractor for Tier Three support.

The Contractor shall provide systems engineering support necessary to establish and maintain a hot-line support capability. The Contractor shall refer technical issues to appropriate technical personnel and provide technical assistance.

The Contractor shall establish a procedure for recording and tracking all requests for operational support. All requests for operational support shall be reviewed and prioritized by the DHS Program Office. The Contractor shall, as a minimum, provide the following support:

1. Provide initial problem resolution where possible.
2. Generate, monitor, and track open Incident Reports through resolution and report the statistics to DHS.
3. Provide software support.
4. Record problem resolution.
5. Maintain frequently asked questions and their resolutions.
6. Obtain customer feedback and conduct surveys.

C.4.6.2 SUBTASK 6.2 – FOC Training

The Contractor shall develop operational training plans and associated training materials, and conduct operational training. The training plans shall outline the personnel to be trained, a schedule for training and shall show graphical representations of the screens of the developed/modified systems. The Contractor shall provide the following:

1. Development of education, training and awareness briefings, and articles.
2. Maintain employee participation status.
3. Prepare security education, training and awareness materials.
4. Provide training to CMaaS vendors.

The Contractor shall develop a training program that addresses proper transmittal of sensor data to the dashboard, how to establish and maintain a dashboard link, basic dashboard operations. The Contractor shall provide the training onsite or at designated locations nationwide, TBD by the COR.

C.4.7 TASK 7 – CDM Acquisition Milestone Tracking System (CLIN X001)

The Contractor shall maintain a system to track the CDM dashboard project as it proceeds through each SELC milestone. This CDM Acquisition Milestone Tracking System shall identify, schedule, and report on the progress of meeting review entrance and exit criteria and completing program artifacts.

The electronic tracking system shall identify all of the required documents for delivery/ presentation to each DHS Review Authority, along with tracking the scheduled start and completion dates and the actual start and completion dates for preparation, review, and approval of each document. The system shall also identify, for each document, the document name and identification number; version number; date; organization; and the specific person in that organization responsible for completing the preparation, review, and approval of each document.

The Contractor shall prepare and deliver a monthly report providing the status of the program's progression through the acquisition milestones. For an FNR-sponsored project that is entering into an acquisition milestone review, the report should include a summary of the status of the required artifacts and indicate which artifacts may require attention prior to the review.

In addition to the DHS acquisition reviews, the Contractor shall support the Government in developing and supporting FNR-internal program capability reviews by providing relevant CDM Acquisition Milestone Tracking System output. These reviews will be performed in preparation for submitting program documents to the Systems Engineering Lifecycle, Enterprise Architecture, and Acquisition Review Boards.

C.4.8 TASK 8 – Testing Support (CLIN X001)

The Contractor shall provide testing support for all scheduled software releases (IOC, FOC, and future updates). The Contractor shall prepare functional testing and coordinate with DHS for system acceptance on all system upgrades and software releases. All results and problems tracked through customer support shall be logged and reported to FEDSIM and DHS upon request and in the monthly report.

The Contractor shall prepare test plans and procedures which shall provide for user acceptance testing of functional enhancements for all major releases of the Dashboard. Major releases shall be identified by incremental increases in either the first or second position of the release number (i.e., 2.0, 2.1, 3.1). Minor releases shall be identified by incremental numbering following the first two positions of the release number (i.e., 2.1.1, 1.1.0.5).

The Contractor shall support the CDM Dashboards by providing interface testing, integration testing, preparation of test plans and procedures, test reports, acceptance testing, and demonstration activities of products targeted for and used by CDM Dashboards.

System testing and laboratory support shall include, but not be limited to, testing support through final acceptance testing of targeted applications; testing for scalability, conducting integration testing of hardware, software, and/or data communications enhancements; and providing support for and liaison with system maintenance, configuration management and control activities for new and existing dashboard applications.

The Contractor shall provide an Integration Test and Evaluation (IT&E) capability that is capable of the development, deployment, and ongoing support of the information systems that now and in the future will comprise the CDM Dashboard.

The Contractor shall establish a testing capability/process and provide support to ensure that all integrated applications are compatible and interoperable with all deployed Dashboard components prior to installation on the Dashboard.

The Contractor shall prepare a Test and Evaluation Master Plan (TEMP) that provides the Contractor's conceptual approach for delivering quality products to include critical test parameters, evaluation criteria, developmental test and evaluation methods, operational test and evaluation methods, automated test tools, and resource management. The Contractor shall identify sets of the testing tools to implement in the test environment. The Government must approve the test plans prior formal testing. The Contractor shall follow this approved Master Plan throughout the task order to produce test plans and reports. The initial TEMP shall be delivered to TPOC and the FEDSIM COR within 30 work days after the Government makes their approach decision.

The Government and/or its representatives (operational test authority [OTA] , Independent Verification and Validation Team [IV&V] for example) shall be allowed to observe any developmental /operational test and evaluation conducted by the Contractor. The Government and/or its representatives (OTA, IV&V etc) shall be able to review the Contractor's test plan(s) with sufficient time to comment and have comments incorporated by the Contractor into the test plan as appropriate. The Contractor is expected to participate in integrated project teams for test and evaluation. The Government reserves the rights to conduct an operational and security related assessments of the Dashboard with users involved, with the full cooperation of the Contractor. Results from these security/operational assessment shall be used to provide feedback to the Government program office as to how the dashboard is proceeding towards meeting security/ operational requirements.

C.4.9 TASK 9 – Configuration Management (CLIN X001)

C.4.9.1 SUBTASK 9.1 – Configuration Management Support

The Contractor shall provide Configuration Management of the Federal and D/A Dashboard systems, to include hardware, software, and networks. The Contractor shall use industry best practices to provide configuration identification, configuration control, configuration status accounting, and configuration review/audit services. The Contractor shall conduct the following configuration management activities as a minimum:

1. Use the appropriate Configuration Management tool to account for changes made IAW the Configuration Management process. The Configuration Management tool shall account for Federal Dashboard assets, software and hardware, and status

accounting to include, as a minimum: Maintain hardware and software accountability and configuration change records for all Federal Dashboard hardware and software assets by make, model, and serial number; Maintenance history; Warranty information; License information; and Configuration change information.

2. Work directly with requesters and technical support personnel to gather sufficient background information to ensure proposed solutions meet customer needs and requirements.
3. Record and report change processing and implementation status throughout the system life-cycle (hardware and software).
4. Ensure proper licensing for software in use on supported systems and networks and maintain a system of licensing accountability and internal control procedures.
5. Provide technical assistance in configuring, testing, and recommending software, hardware, and network management utilities.

C.4.9.2 SUBTASK 9.2 – Prepare Configuration Management Plan

The Contractor shall prepare a Configuration Management Plan to identify and define the organization and responsibilities, overall tasks, principles, and configuration management processes for the Dashboard. The purpose of Configuration Management Plan is to ensure a coherent view of a compatible method and procedure for configuration management of the system and its comprising subsystems, and provide emphasis on a disciplined integrated configuration management approach. The Configuration Management Plan shall establish the processes to manage changes in documentation, systems, hardware configuration items, and software configuration items. It shall define the Configuration Management organization and responsibilities, define the baselines to be tracked, and address the four major activities of Configuration Management: configuration identification, configuration control, configuration status accounting, and configuration auditing functions. The Contractor shall provide this CM support in conjunction with the Government Change Control Boards (CCBs) at the Federal and D/A levels.

C.4.10 TASK 10 – Software Changes (CLIN X001)

The Contractor shall provide on-going support to maintain and improve the functional processes within Dashboard software as prioritized and approved by DHS and the FEDSIM COR. These requirements shall consist of maintenance requirements, feature clarifications, modifications, and deficiency reports submitted and prioritized and approved by DHS. The Contractor shall provide support for all phases of project life cycle, including analysis, design, and program code, testing, and implementation, for the approved Dashboard maintenance, feature clarifications, modifications, and approved deficiency requests. The Contractor shall conduct and/or participate in design approval reviews and provide documentation updates to reflect functional and operational impacts and alternatives. All changes will have to be reviewed including COTS/Open Source Code software patch and revision updates. The Contractor shall provide a software version release every six months, or as required by the Government.

C.4.11 TASK 11 – Contractor Acquired Property (CLINs X001 and X005)

The Contractor shall acquire IOC Dashboard IT assets, e.g., equipment, software, and services in support of the IOC Dashboard. Upon receipt of Government approval, the following categories of information technology assets shall be procured by the Contractor: software, hardware, upgrades, licenses, and spare parts as required, in accordance with the terms of paragraph H.5 of the Alliant SB basic contract. The Contractor shall ensure that all hardware provided includes the most cost-effective warranty available from the vendor. In most cases, warranty coverage should be for parts only versus on-site warranty coverage.

C.4.12 TASK 12 – Source, Object, Executable and Run-time Code (CLIN X001)

The Contractor shall provide the most current version(s) of any and all source, object, executable and run-time code (as applicable) developed under the efforts of this contract ("New Code") for the IOC and FOC Dashboard Solutions and unique enhancements, customization/plug-ins/etc ("Customizations") to the Government in accordance with the delivery requirements in section F.5. The Government's requirements for data rights in the New Code and Customizations are specified in sections H.25.6, H.26, H.27, L.8.7 and M.5.1(c) and FAR clause at 52.227-17, Rights in Data – Special Works (Jun 1987). The Contractor shall ensure that all COTS licenses, and Open Source licenses both allow for the creation of the New Code and Customizations and vest the data rights to the New Code and Customizations exclusively in the Government, in both cases without additional charge to the Government. DHS will have unlimited rights to use and modify all source, object, executable and run-time code (as applicable) comprising the New Code and Customizations, and its associated documentation, even in the event that the Contractor should become unable to continue supporting the Dashboard, and the Contractor shall deliver each deliverable accompanied by a signed assignment of copyright to the Government as contemplated under the FAR clause at 52.227-17, Rights in Data – Special Works (Jun 1987). Source, object, executable and run-time code (as applicable) comprising the New Code for releases of the software produced under this contract shall become the property of the Government upon termination of the contract. The source, object, executable and run-time code (as applicable), with their associated documentation and other materials as specified in section F.5, shall be delivered to DHS on dates established in accordance with section F.5, but in any event no later than 30 calendar days following the termination/expiration of the contract. In the event the Contractor defaults on the terms of this contract for any reason, the most current version of the source, object, executable and run-time code shall be delivered to DHS no later than 30 calendar days following the event that leads to the termination/expiration of the contract and the Government will retain the right to use any and all versions that are at that time installed at a Government facility, and to further develop and distribute them, with no further royalties or other payments being due to the Contractor or any other party.

C.4.13 TASK 13 – Transition to Support Plan (CLIN X001)

The Contractor shall develop and deliver a Transition to Support Plan that documents how the FOC Dashboard solution will be operated and supported (once it is transitioned to the Government and/or a third party who will be operating and maintaining it). The FNR Operations group will manage the transition to support process for the Government. The Transition to Support Plan shall address the following:

1. Deployment schedule/milestones.
2. Required support resources.
3. Deployment tasks that require system administration support.
4. Security “clean bill of health” (required scan results, remediation POA&Ms, etc.).
5. Detail DHS Technical Reference Model (TRM) actions.
6. System architecture diagram(s).
7. Testing Results.
8. Readiness Activities.
9. Training resources.
10. System demonstrations.

L.1 52.252-1 SOLICITATION PROVISIONS INCORPORATED BY REFERENCE (FEB 1998)

This solicitation incorporates one or more solicitation provisions by reference, with the same force and effect as if they were given in full text. Upon request, the CO will make the full text available. The offeror is cautioned that the listed provisions may include blocks that must be completed by the offeror and submitted with its quotation or offer. In lieu of submitting the full text of those provisions, the offeror may identify the provision by paragraph identifier and provide the appropriate information with its quotation of offer. The solicitation provisions and/or contract clauses are available in either HTML or PDF format at:

https://www.acquisition.gov/far

Clause No	Clause Title	Date
52.215-1	Instructions to Offerors-Competitive Acquisition	(JAN 2004)
52.215-20	Requirements for Cost or Pricing Data or Information Other Than Cost or Pricing Data – Alternate IV	(OCT 2010)
52.232-38	Submission of Electronic Funds Transfer Information with Offer	(MAY 1999)

L.2 GENERAL INSTRUCTIONS

a. Offerors shall furnish the information required by this solicitation. A Standard Form (SF) 33, "Solicitation, Offer, and Award," completed and signed by the offeror, Block 17 constitutes the offeror's acceptance of the terms and conditions of the proposed TO. Therefore, the SF 33 must be executed by a representative of the offeror authorized to commit the offeror to contractual obligations.

b. Offerors are expected to examine this entire solicitation document including the Contract. Failure to do so will be at the offeror's own risk.

c. The Government may make award based on initial offers received, without discussion of such offers. Proposals shall set forth full, accurate, and complete information as required by this solicitation package (including Attachments). The penalty for making false statements in proposals is prescribed in 18 U.S.C. 1001.

d. Offerors submitting restrictive data will mark it as follows in accordance with the FAR 52.215-1, Instructions to Offerors-Competitive Acquisition, which is incorporated by reference. Clause 52.215-1 states: "Offerors who include in their proposals data they do not want disclosed to the public for any purpose or used by the Government except for evaluation purposes, shall –

   Mark the title page with the following legend:

   > "This proposal includes data that shall not be disclosed outside the Government and shall not be duplicated, used or disclosed--in whole or in part--for any purpose other than to evaluate this proposal or quotation. If, however, a Task Order is awarded to this offeror as a result of--or in connection with--the submission of this data, and the Government incorporates the proposal as part of the award, the Government shall

have the right to duplicate, use, or disclose the data. Also, this restriction does not limit the Government's right to use information contained in this data if it is obtained from another source without restriction. The data subject to the restriction is contained in sheets (insert numbers or other identification of sheets)"; and

Mark each sheet of data it wishes to restrict with the following legend:

"Use or disclosure of data contained on this sheet is subject to the restriction on the title page of this proposal or quotation."

e. The Government assumes no liability for disclosure or use of unmarked data and may use or disclose the data for any purpose. Unless restricted, information submitted in response to this request may become subject to disclosure to the public pursuant to the provisions of the Freedom of Information Act (5 U.S.C. 551).

f. The authorized negotiator or the signatory of the SF 33 will be notified of the date and time of the oral technical proposal presentation. Offerors shall provide the name of the individual, the position title, telephone number, fax number, and electronic mail address of that individual.

g. This procurement is conducted under the procedures of FAR Subpart 16.5. The policies and procedures of FAR Subpart 15.3 do not apply.

L.3 SUBMISSION OF QUESTIONS

Offerors are requested to submit their questions grouped by solicitation Section and make reference to the particular Section/Subsection number. Questions must be received before the date specified for receipt of questions. **Questions or requests for extension submitted after the cut-off date will not be considered.**

Any information given to a prospective offeror concerning this solicitation will be furnished promptly to other prospective offerors as an amendment to the solicitation.

L.4 AVAILABILITY OF EQUIPMENT AND SOFTWARE

All commercial hardware and software proposed in response to this solicitation document shall have been formally announced for general release on or before the closing date of the solicitation. Failure to have equipment or software announced prior to submission of proposal may render the offeror’s proposal unacceptable.

L.5 GENERAL INFORMATION

The total estimated CPAF of the TO is between $43.6 million and $48.4 million**,** including all transition costs, fees, ODCs, and Travel.

L.6 SUBMISSION OF OFFERS

Each offer shall be in three parts.

The offeror shall submit all on the due date indicated on SF 33.

Part I is the written Cost/Price proposal and shall contain the following:

- Solicitation, Offer and Award (SF33) (TAB A)

- Section B – Supplies or Services and Prices/Costs (TAB B)
- Cost/Price Supporting Documentation (TAB C)
- Subcontractor Supporting Documentation (TAB D)
- Cost/Pricing Assumptions (TAB E)
- Organizational Conflict of Interest Statement (TAB F)
- Contract Registration (TAB G)
- Current Forward Pricing Agreements (TAB H)
- Management Systems (TAB I)
- Cost Accounting Standards (CAS) Disclosure Statement (D/S) (TAB J)
- Unique Labor Categories (TAB K)

Part II is the written Technical Proposal and shall contain the following:

- Project Staffing Plan Table (This item contains documentation that will be used to make a Pass/Fail determination in accordance with TOR Section M.5.)
- Key Personnel Qualification Matrix, including Letters of Commitment (This item contains documentation that will be used to make a Pass/Fail determination in accordance with TOR Section M.5.)
- Draft Quality Control Plan (This item contains documentation that will be used to make a Pass/Fail determination in accordance with TOR Section M.5.)
- Draft Earned Value Management Plan
- Section 508 Compliance Statement. (This item contains documentation that will be used to make a Pass/Fail determination in accordance with TOR Section M.5.)
- Technical Assumptions (if any)
- Data Rights Continuity Plan
- Copy of Oral Technical Presentation Slides

Part III is the oral technical proposal presentation and shall contain the following:

- Technical Approach
- Management Approach
- Key Personnel and Project Staffing
- Corporate Experience

The CO will schedule the oral technical proposal presentation after all proposals are received. The oral technical proposal presentation shall contain the information shown in paragraph L.10.

L.7 SUBMISSION OF THE WRITTEN COST/PRICE PROPOSAL (PART I)

Audits may be performed by Defense Contract Audit Agency (DCAA) on the offeror and all subcontracts. Cost/Price Proposals shall meet the DCAA audit submittal requirements. Cost proposals will be evaluated (but not scored) based on a Cost Realism Analysis. Offerors shall fully support all proposed costs. An offeror's proposal is presumed to represent the offeror's best efforts in response to the solicitation. Any inconsistency, whether real or apparent, between promised performance, and cost or price, shall be explained in the proposal.

Offerors shall provide adequate information to allow the Government to perform a Cost Realism analysis. Pursuant to FAR 2.101, Cost Realism is defined as:

> "…the process of independently reviewing and evaluating specific elements of each offeror's proposed cost estimate to determine whether the estimated proposed cost elements are realistic for the work to be performed; reflect a clear understanding of the requirements; and are consistent with the unique methods of performance and materials described in the offeror's technical proposal."

Written Cost/Price Proposals shall be submitted as an original, (1) paper copies, and an electronic copy. The offeror shall submit all proposed costs using Microsoft Excel software utilizing the formats without cells locked and include all formulas. The offeror shall submit information sufficient to enable the following types of review:

a. Indirect Rate Review: The offeror shall break out all proposed indirect rates (unburdened), by contract line item, and by each fiscal year. The offeror shall clearly identify the cost base in which all indirect rates are applied. If the offeror has an approved Forward Pricing Rate Agreement (FPRA), adequate proof of this approval shall be provided. Additionally, the offeror's cognizant DCAA auditor's name and phone number shall be included in the cost proposal. Historical indirect rates (unburdened) shall be provided (Overhead, Fringe, General and Administrative, etc.) for the last five years inclusive of appropriate explanations for any major increases and decreases in the rates between years. Offerors without audited rates shall propose indirect rates in accordance with FAR Part 31.

b. Direct Labor Rate Review: The offeror shall include the base labor rate (unburdened) for all proposed labor categories and all projected rates for all out years. The Key Personnel labor rates shall be supported by evidence of actual rates currently being paid for non-Key Personnel (e.g., actual labor rates for like positions). Additionally, the offeror shall include any information that may be available to support the reasonableness of all direct labor rates proposed. The offeror shall identify all direct labor escalation factors. Offerors shall include a cross-walk of its labor categories, basis of cost element, weightings, and explanations to those in the solicitation (e.g., used category average rates of xxx and yyy categories dated xx February 2011 with 40% and 60% weightings respectively). If GSA Schedule labor rates are utilized, provide the cross-walk and copy of GSA Schedule contract.

c. Award Fee Review: The offeror shall break out all proposed award fees and clearly delineate the cost base in which the fee percentages are applied.

d. Comparison of Total Proposed Cost to the Government Independent Cost Estimate (IGCE): The Government will use the IGCE as an informational tool by comparing this estimate to the offeror's total proposed cost.

All prime offerors are responsible for ensuring that all subcontracts include the same type of cost detail as required above.

Pursuant to Section L.6 (Submission of Offers Section), offerors shall not include any cost data in the technical, management, or past performance proposals.

L.7.1 COST/PRICE PROPOSAL TABS

The proposal shall contain the following tabs:

a. Solicitation, Offer and Award (SF 33) (Tab A). When completed and signed by the offeror constitutes the offeror's acceptance of the terms and conditions of the proposed Task Order. Therefore, the form must be executed by representatives of the offeror authorized to commit the offeror to contractual obligations. Offerors shall sign the SF 33 in Block #17.

b. Section B – Supplies or Services and Prices/Costs (Tab B). The offeror shall indicate the price to be charged for each item in Section B rounded to the nearest whole dollar.

c. Cost/Price Supporting Documentation (Tab C). The information requested in the proposal is required to enable the Government to perform cost or price analysis. The offeror shall prepare one summary schedule (Section B) which provides the Total Not-To-Exceed Amount for each CLIN and the Total Not-To-Exceed Price offered. Along with the summary schedule, the offeror is required to provide full back-up documentation for each CLIN and proposed Task Area. The back-up documentation shall detail the labor categories to be used, labor hours proposed by category, material and equipment costs, and a total cost breakdown (to include a summary total for each cost component, e.g., labor, overhead, or G&A).

d. Subcontractor Supporting Documentation (Tab D). The offeror shall also provide supporting cost/price documentation for all proposed subcontractors, to include the proposed type of subcontract and if the contract with the subcontractor is a Time and Material provide justification. In addition to the cost back-up documentation, Defense Contract Audit Agency contact information and relevant cost/pricing data shall be provided for all subcontractors. Failure to provide complete supporting documentation may result in no further consideration of the offeror's proposal. Subcontractors may submit proprietary data directly to the Contracting Officer or through the prime Contractor in a separate, sealed envelope.

e. Cost/Pricing Assumptions (Tab E). Offerors must submit, under a separate tab, all (if any) assumptions upon which the Cost/Price Proposal is based.

f. Organizational Conflict of Interest Statement (Tab F). The offeror shall complete and sign an Organizational Conflict of Interest Statement in which the offeror (and any subcontractors, consultants or teaming partners) disclose information concerning actual or potential organizational conflict of interest affecting the offeror's proposal or any work related to this TOR. The statement shall be accompanied by the offeror's plan for mitigation, avoidance, or neutralization, if appropriate.

g. Contract Registration (Tab G). The offeror shall submit a statement that the contract vehicle under which this proposal is being submitted has been registered in TOS and that all information in TOS is up-to date.

h. Current Forward Pricing Agreements (Tab H). The offeror shall submit all forward pricing agreements including that of the Prime Contractor, Subcontractors, Teaming Partners, Reorganizations & Mergers.

i. Management Systems (Tab I). The offer shall describe all applicable management systems (e.g., accounting, estimating, purchasing, EVMS). The offeror shall include the date of the last audit, results of the audit, audit report number, and date determined adequate.

j. Cost Accounting Standards (CAS) Disclosure Statement (D/S) (Tab J). The offeror shall include a copy of the CAS D/S. Also, the offer shall state the adequacy of D/S, when audited, audit report number, when determined adequate by ACO, and include any non-compliances with CAS.

L.8 SUBMISSION OF THE WRITTEN TECHNICAL PROPOSAL, PART II

Each offeror shall submit all information described in the following paragraphs. The offeror shall provide 5 **electronic copies** containing all required sections of this Part.

L.8.1 PROJECT STAFFING PLAN TABLE

The Offeror shall provide a Project Staffing Plan Table in accordance with the Project Staffing Plan Table Template (Section J, Attachment N). The submission shall contain all individuals that will be working on this effort. All Key Personnel proposed shall be available to begin work immediately on the Project Start Date indicated in Section F.5 of this solicitation.

The Offeror shall represent the following:

a. All personnel assigned to this TO will meet the requirements of the Alliant Small Business Contract prior to assignment.

b. All personnel assigned to this TO will meet the requirements of the TO prior to starting work.

If the names of all non-Key Personnel are not known prior to offer submission, the Offeror may indicate "to be determined" in the Project Staffing Plan Table. The names of non-Key Personnel are the only identifiers that may remain unspecified in the Project Staffing Plan Table. The names of all non-Key Personnel that can be provided shall be provided.

L.8.2 KEY PERSONNEL QUALIFICATION MATRIX

The Offeror shall submit a Key Personnel Qualification Matrix (in the format provided in Section J, Attachment H) for each Key Person proposed relating the specialized experience identified in Section H.2 of this TO and the qualifications of the person or persons being proposed for that position. For those additional Key Personnel proposed, the Offeror shall identify the specialized experience and the corresponding qualifications for this experience. Each Key Personnel Qualification Matrix shall be limited to 3 pages.

The Offeror shall represent the following:

a. All Key Personnel named are available to begin work on the Project Start Date designated in Section F.

b. Letter of Commitment, signed by each proposed Key Person at the proposal submission due date.

L.8.3 DRAFT QUALITY CONTROL PLAN

This shall be limited to 15 pages.

The Offeror's Draft Quality Control Plan (QCP) shall describe its quality control methodology and proposed performance metrics.

The Offeror shall discuss the following elements:

a. Approach to planning, organizing and managing of internal resources and subcontractors, to include lines of authority.
b. Methods for tracking and reporting progress and costs and integrating the requirements of the TO.
c. Identification of and resolution of issues and problems, including escalation procedures.

L.8.4 DRAFT EARNED VALUE MANAGEMENT PLAN

This shall be limited to 15 pages.

The Offeror's Draft Earned Value Management Plan shall describe its proposed methodology to employ and report on EVM in the management of this TO.

The Offeror shall discuss the following elements:

a. Providing the Updated Earned Value Management Plan at the Kick-Off meeting:

b. Compliance with TOR H.19, Earned Value Management reporting requirements.

c. Employing EVM in the management of this TO in accordance with the American National Standards Institute (ANSI)/Electronic Industries Alliance (EIA) Standard-748-A-1998, *Earned Value Management Systems.*

d. Application of EVM techniques to this TO in accordance with FAR 34.201 and industry best practices.

e. The Integrated Baseline Reviews and the Contractor's approach to jointly assess planning, logical scheduling of the work activities, adequate resources, and identification of inherent risks.

L.8.5 SECTION 508 COMPLIANCE REQUIREMENTS

The Offeror's written proposal shall include a statement indicating its capability to comply with Section 508 requirements throughout its performance of this TO in compliance with Section H.14. The Offeror's proposal will be evaluated to determine whether it includes a statement indicating its capability to comply with Section 508 requirements throughout its performance of this TO. Any proposal that does not include a statement indicating the Offeror's capability to comply with Section 508 requirements throughout its performance of this TO shall be eliminated from further consideration for award.

L.8.5 TECHNICAL ASSUMPTIONS

Offerors shall identify and address any assumptions affecting the technical proposal citing the component(s) of the proposal to which they pertain.

The Government reserves the right to reject any proposal that includes any assumption that adversely impacts the Government's requirements.

L.8.6 DATA RIGHTS CONTINUITY PLAN

Offerors shall describe their plan for delivering COTS and/or Open Source software and hardware, Customizations and New Code with sufficient data rights to meet the requirements of this TOR, including without limitation the requirements set forth in sections C.4.12 and H.25. The plan shall also address the preservation of open source and/or commercial software, and the Government's access thereto, in the event of a termination or expiration of this TO or a material adverse event affecting the ability of the licensor to continue providing such software, by means of a public or private third-party escrow arrangement, conditional on Government approval. For open source software, the Government will look more favorably on Open Source software provided with an acknowledgment-type license such as BSD (Berkeley Source Distribution) type license. This plan will be evaluated as part of the offeror's Technical Approach.

L.9 DELIVERY INSTRUCTIONS

Offerors shall deliver written proposals and receive acceptance from:

General Services Administration
Attn: Millicent Hawkins (GSA FEDSIM)
GSA/FAS/AAS/FEDSIM
1800 F Street NW
Washington, DC 20405
(703) 605-3654
(703) 589-7747 (c)

Proposals not received by 11:00 a.m. Eastern Time (ET) on the date stated in the TOR cover letter will not be considered.

L.10 PART III – ORAL TECHNICAL PROPOSAL PRESENTATION

Each offeror shall make an oral technical proposal presentation and participate in a question and answer (Q&A) session led by the CO and participated in by the Technical Evaluation Board (TEB) Members and other representatives of the Government. The offeror must be prepared to answer questions about the oral technical proposal presentation and the written technical proposal in the Q&A session. The oral technical proposal presentation and Q&A session will be held at the unclassified level. The oral technical proposal presentation will be used to assess the offeror's capability to satisfy the requirements set forth in the TOR. The offeror's oral technical proposal presentation shall contain the information in Section L.10 The contents of all proposals will be delivered to FEDSIM at the same time. The oral technical proposal presentation, Part III, shall be separately bound from Parts I and II.

Oral technical proposal presentation slides presented that differ from slides delivered with the technical proposal will not be evaluated. The TEB will review the offerors Oral Slides at the same time they review the offerors Written Technical proposal.

L.10.1 ORAL TECHNICAL PROPOSAL PRESENTATION PARTICIPATION

Reserved

L.10.2 ORAL TECHNICAL PROPOSAL PRESENTATION CONSTRAINTS

The offeror shall identify the authors of the presentation by name and association with the offeror. Attendance at the presentation and the subsequent Q&A session shall be limited to the offeror's Key Personnel (all Key Personnel are highly encouraged to attend) and no more than three additional corporate representatives of the offeror. An offeror's "Key Personnel" includes only those persons who will be assigned to the TO as Key Personnel as described in Section H.2. The three additional people (e.g., CEOs, company presidents, or contract representatives) from the offeror may attend, but will not be allowed to participate in the presentation. Any of the three additional personnel may make a brief introduction which will not be evaluated, but will count towards the offeror's allotted time. For the remainder of the presentation, only Key Personnel shall present.

The offeror will be given 15 minutes for set up. After opening remarks by the Government, the offeror will be given up to 120 minutes to present. The presentation will be stopped precisely after 120 minutes. The Offeror shall allow for a 10 minute break (which will not count as part of the allotted 120 minutes) at approximately the halfway point in the presentation. The exact time for this break shall be at a logical breaking point to be determined by the Offeror.

Upon completion of the presentation, the Government will caucus to formulate any clarification questions regarding the technical proposal, however, unless specifically requested by the Contracting Officer, proposal revisions are not expected and will not be allowed. The Government and offeror will then address any clarification questions posed by the CO or the TEB Chairman. The offeror may briefly caucus to coordinate responses to specific requests clarifications.

The offeror can expect to spend up to half a day through the total presentation, caucus, and clarification session. The CO and the TEB Chairman will be responsible for ensuring the schedule is met and that all offerors are given the same opportunity to present and answer questions. **Offerors shall provide 8 appropriately bound hard copies of the presentation materials (including slides, transparencies).** Only those slides actually presented and talked to will be considered in the technical evaluation.

L.10.3 ORAL TECHNICAL PROPOSAL PRESENTATION MEDIA

The number of slides that can be presented during the oral technical proposal will be limited to 150. Only those slides presented, and talked about during the oral presentation will be considered for evaluation (oral technical proposal presentation slides shall be submitted in advance with the written submission). Any slides over and above those presented, and talked about during the oral presentation will be returned to the offeror and will not be evaluated as part of this source selection. No other media may be used. Presentation media is limited to computer-based graphics of the offeror's choice or normal viewgraph slides displayed using an appropriate projector. Unobtrusive company logos or names can be inserted in any or all slides. Slides should be sequentially numbered in the lower right corner. Transition effects shall not be used. The slides shall not contain any fonts smaller than a proportionally spaced font (such as Times New Roman) of at least 12 point.

Except for the screen provided in the conference room, the Government will provide no equipment. The offeror shall be responsible for any equipment necessary for the presentation.

L.10.4 ORAL TECHNICAL PROPOSAL PRESENTATION SCHEDULING

The CO will schedule the oral technical proposal presentation with the authorized negotiator or the signatory of the SF 33. Time slots will be assigned randomly and may not be changed or traded. The Government reserves the right to reschedule any offeror's oral technical proposal presentation at its sole discretion.

Oral Technical Proposal Presentations will be given at facilities designated by the CO. The exact location, seating capacity, and any other relevant information will be provided when the presentations are scheduled.

L.10.5 RECORDING OF THE ORAL TECHNICAL PROPOSAL PRESENTATION

The offeror may **not** record or transmit any of the oral presentation process. All offeror's electronic devices shall be removed from the room while the Government is caucusing after the oral presentation.

L.10.6 ORAL TECHNICAL PROPOSAL PRESENTATION TOPICS

The Government does not expect the offeror to provide a thorough presentation of those items already submitted in writing in Part II. Instead, the offeror shall address this information under the topics provided. The oral technical proposal presentation shall include the following topics, and be organized in the following order:

a. Topic 1: Technical Approach
b. Topic 2: Management Approach
c. Topic 3: Key Personnel and Project Staffing
d. Topic 4: Corporate Experience

L.10.6.1 TECHNICAL APPROACH (TOPIC 1)

The Offeror's technical approach shall demonstrate its capabilities, expertise, and experience by discussing their Technical Approach in the following areas:

a. Understanding of the DHS Dashboard objectives and the .gov Continuous Monitoring and Diagnostics operational, technical, and regulatory environment.
b. The Offeror's approach to meeting DHS and D/A security requirements (to include security accreditation of the CDM Dashboard Solution).

c. The Offeror’s methodology and processes guiding the performance of the technical requirements identified in Section C of this TOR (to include the DHS EA and SELC processes and an approach to meeting all DHS review requirements). This includes a general description of how the technical approach will be applied to accomplishing the task requirements and meeting the performance metrics.
d. Understanding of the current Commercial Dashboard Technology and capabilities and methodology to analyze alternative products.
e. The Offeror shall describe their approach to protect against supply chain threats to the Dashboard (as defined in the NIST 800-53 SA-12 control) to include a description of what safeguards they intend for supply chain protections.

f. The Offeror’s approach to delivering COTS/Open Source Code software and hardware, New Code and Customizations with sufficient data rights to meet the requirements of this TOR, including without limitation the requirements set forth in sections C.4.12 and H.25.

L.10.6.2 MANAGEMENT APPROACH (TOPIC 2)

The Offeror’s Management approach shall demonstrate their capabilities, expertise, and experience by discussing the following:

a. Methodology for establishing the working relationship required to interface with the CMaaS Contractor from testing through installation and ongoing support. This includes how the Offeror will communicate and collaborate with the DHS Operational Test Authority (OTA) and any CMaaS vendor(s) or other Government-designated integrators responsible for the installation of the Dashboard at the specific D/As site.
b. The Offeror’s Baseline/Change Request methodology and processes to provide timely maintenance/enhancement of the dashboard.
c. The Offeror’s methodology and processes to manage the performance of the technical requirements identified in Section C of this TOR and the performance metrics in the AFDP (to include Offeror-proposed metrics).
d. The Offeror's approach to risk management and the planned actions to mitigate or eliminate the risks.
e. The Offeror’s approach/process for clear lines of communication between the Contractor’s team and the Government, for timely problem identification, mitigation, and resolution.
f. The Offeror’s mature software development processes (e.g. CMMI Level 3 (minimum) Certification for entire company or the portion of the company that will be working on this Task Order).
g. Approach to planning, organizing and managing of internal resources and subcontractors, to include lines of authority.

h. Methods for tracking and reporting progress and costs and integrating the requirements of the TO.

L.10.6.3 KEY PERSONNEL AND PROJECT STAFFING (TOPIC 3)

During the oral presentation, the Offeror shall discuss its project staffing approach, describing the project staffing strategy and the rationale for the proposed labor mix. The Offeror shall specifically address rationale for choosing specific Key Personnel. The Offeror shall describe how each Key Person would be involved in each task/subtask and how their qualifications and experience uniquely qualify them for the Key Personnel positions described in Section H.

L.10.6.4 CORPORATE EXPERIENCE (TOPIC 4)

The Offeror shall discuss its Corporate Experience performed/managed by the Prime Contractor bidding on this effort, within the last five years, that reflects/identifies experience on three projects that are similar in scope and complexity to the requirements contained in Section C of the TOR and the functional requirements (Section J, Attachments B and C). The Offeror shall discuss the scope of work, the period during which the work occurred, the dollar value of the work performed, the client and project, the specific responsibilities of the Offeror, major deliverables produced, performance measures/service levels applied, and any problems or issues that occurred and the corrective action taken. At least one of these three projects shall demonstrate the Offeror (prime Contractor) experience implementing CMMI Level 3 software development projects.

M.1 METHOD OF AWARD

The Government anticipates awarding a TO to the offeror whose proposal is the most advantageous to the Government, price and other factors considered. Technical proposals will be evaluated based on the factors described in Section M.5. All evaluation factors other than cost or price, when combined, are significantly more important than cost. Award may be made to other than the lowest priced, technically acceptable proposal.

This acquisition is being conducted under FAR 16.5. Principles and procedures of Subpart 15.3 do not apply. The Government may make award based on initial offers received in accordance with FAR clause 52.215-1(f). The Government may consider the offeror's clarifying response(s) without allowing proposal revisions.

After an offeror has been selected for award based upon a best value determination, the Government may negotiate a final reduced price. The negotiations may include reductions in profit/fee with the offeror selected for award in order to achieve the absolute best value for the Government.

M.2 COST/PRICE PROPOSAL EVALUATION

The offeror's written cost proposals (Section L.7, Part I, Tabs A through J) will be evaluated to determine cost realism and reasonableness. Costs that are excessively high or low (without sufficient justification) may be considered unrealistic and unreasonable and may receive no further consideration. Any proposal that is not within the total estimated ceiling cited in Section B and in Section L.5 for the applicable CLINs shall include an explanation that specifically draws the Government's attention to any unique technical aspects of the proposal the offeror would like the Government to consider as the justification for the deviation from the range.

M.3 ORGANIZATIONAL CONFLICT OF INTEREST

Tab F will be evaluated to assess whether or not an actual or potential OCI exists as defined by FAR Part 9.5. If an actual or potential conflict of interest is identified that cannot be mitigated, avoided, or resolved in accordance with FAR Part 9.5, that offeror may be ineligible for award.

M.4 COST ASSUMPTIONS

The Government reserves the right to reject any proposal that includes any cost assumptions that may adversely impact satisfying the Government's requirements.

M.5 TECHNICAL EVALUATION FACTORS

<u>Pass/Fail Elements:</u>
The following will be evaluated on a Pass/Fail basis:

- The Government will reject any proposal that does not provide a name for each Key Person proposed at the proposal submission due date. A proposal that states, "To Be Determined" (TBD) for a proposed Key Person, or omits a Key Person, will be rejected by the Government (Section L.8.2).
- The Government will reject any proposal that does not provide a Letter of Commitment, signed by each proposed Key Person who is not currently employed by the

Prime/Subcontractor, i.e., Contingent Hires, at the proposal submission due date (Section L.8.2).

- The Government will reject any proposal that does not provide the required personnel representations. (See Sections L.8.1 and L.8.2).
- The Government will reject any proposal that does not provide a Section 508 Compliance Statement (Section L.8.4).

The Government will evaluate technical proposals based on the Factors shown below. The various elements constituting a factor (usually appear as numbered paragraphs (a) through (x)) are not subfactors and will not be separately rated but will be evaluated as a whole to arrive at a factor rating. The technical proposal evaluation Factors are listed in descending order of importance. The TEB will evaluate the oral and written submissions to arrive at a rating for the technical proposal as a whole. The Government will evaluate technical proposals (Section L.8, Part II and L.10.6, Part III) based on the following factors.

The technical proposal evaluation factors are listed in descending order of importance. All 4 technical factors combined are significantly more important than cost. The Government will combine the results of the written and oral submissions to arrive at a rating for the technical evaluation factors as a whole. The receipt of an evaluation rating of Not Acceptable in any single Factor may result in the overall proposal being determined Not Acceptable and therefore ineligible for award. **A failure on any single Pass/Fail criteria will make the proposal ineligible for award, with no further evaluation of the technical and pricing proposal accomplished by the Government.**

M.5.1 FACTOR 1: TECHNICAL APPROACH

The Offeror will be evaluated on the clarity and completeness of the approach and the degree to which the proposal meets the requirements of the TOR Sections L.10.6.1 and L.8.6 and includes effective and efficient methodologies.

a. Understanding of the DHS Dashboard objectives and the .gov Continuous Monitoring and Diagnostics operational, technical, and regulatory environment.
b. The Offeror’s approach to meeting DHS and D/A security requirements (to include security accreditation of the CDM Dashboard Solution).
c. The Offeror’s methodology and processes guiding the performance of the technical requirements identified in Section C of this TOR (to include the DHS EA and SELC processes and an approach to meeting all DHS review requirements). This includes a general description of how the technical approach will be applied to accomplishing the task requirements and meeting the performance metrics.
d. Understanding of the current Commercial Dashboard Technology and capabilities and methodology to analyze alternative products.

e. The Offeror shall describe their approach to protect against supply chain threats to the Dashboard (as defined in the NIST 800-53 SA-12 control) to include a description of what safeguards they intend for supply chain protections (which could include only using signed software).

f. The Offeror's approach to delivering COTS and/or Open Source software and hardware, New Code and Customizations with sufficient data rights to meet the requirements of this TOR, including without limitation the requirements set forth in sections C.4.12 and H.25. The Government will disfavor (e.g., rate as a weakness or significant weakness) any solution that locks the Government into restrictive proprietary languages/platforms that impair the Government's ability to further use, develop, or distribute the Dashboard solution over time as contemplated in this solicitation. The Government's evaluation of the data rights compliance plan will include the following: (1) An assessment of the proposer's approach's providing complete assurance that the goal will be achieved; (2) An assessment of the ability to maintain the approach over time; (3) An assessment of any limitations on the Government's ability to use the software for its intended purpose and on its ability to share the resulting software with others; and (4) Complexity of administration of the approach by Government personnel.

M.5.2 FACTOR 2: MANAGEMENT APPROACH

The Government will evaluate the Management approach factor based on how well the Offeror demonstrates their capabilities, expertise, and experience by discussing the following:

a. Methodology for establishing the working relationship required to interface with the CMaaS Contractor from testing through installation and ongoing support. This includes how the Offeror will communicate and collaborate with the DHS Operational Test Authority (OTA) and any CMaaS vendor(s) or other Government-designated integrators responsible for the installation of the Dashboard at the specific D/As site.

b. The Offeror's Baseline/Change Request methodology and processes to provide timely maintenance/enhancement of the dashboard.

c. The Offeror's methodology and processes to manage the performance of the technical requirements identified in Section C of this TOR and the performance metrics in the AFDP (to include Offeror-proposed metrics).

d. The Offeror's approach to risk management and the planned actions to mitigate or eliminate the risks.

e. The Offeror's approach/process for clear lines of communication between the Contractor's team and the Government, for timely problem identification, mitigation, and resolution.

f. The Offeror's mature software development processes (e.g. CMMI Level 3 (minimum) Certification for entire company or the portion of the company that will be working on this Task Order).

g. Approach to planning, organizing and managing of internal resources and subcontractors, to include lines of authority.

h. Methods for tracking and reporting progress and costs and integrating the requirements of the TO.

The Government will evaluate the Management approach factor based on the clarity and completeness of the approach and the degree to which the proposal meets the requirements of the TOR (in particular those areas described in Sections L.10.6.2, L.8.3 and L.8.4).

M.5.3 FACTOR 3: KEY PERSONNEL AND PROJECT STAFFING

The project staffing plan will be evaluated to assess the degree to which it complies with the requirements outlined in Section L.8.1 and Section L.10.6.3, including the estimated hours and labor mix (for both Key and non-Key Personnel). The Key Personnel will be evaluated to assess the appropriateness and completeness of the experience, skill and qualifications of the proposed Key Personnel in accordance with Section H.2 and Section L.8.2.

M.5.4 FACTOR 4: CORPORATE EXPERIENCE

The Corporate Experience factor will be evaluated based on the degree to which the Offeror meets the requirements described in Section L.10.6.4 and the following:

a. Corporate experience reflects/identifies experience on projects that are similar in scope, size and complexity to the requirements contained in Section C of the TOR and the functional requirements (Section J, Attachments B and C).
b. Corporate experience submission provides information which provides the Government confidence that the Offeror can successfully perform the work of this TOR.
c. Offeror's (the prime Contractor) experience implementing CMMI Level 3 software development projects.

M.4 TECHNICAL ASSUMPTIONS

All technical assumptions will be reviewed in the context of the technical factor to which they apply. The Government reserves the right to reject any proposal that includes any technical assumption that may adversely impact satisfying the Government's requirements.